Title	A Modified Completeness Theorem of KAT and Decidability of Term Reducibility(Digest_要約)
Author(s)	Uramoto, Takeo
Citation	Kyoto University (京都大学)
Issue Date	2014-03-24
URL	http://dx.doi.org/10.14989/doctor.k18041
Right	学位規則第9条第2項により要約公開; 許諾条件により要約は2015-03-23に公開
Type	Thesis or Dissertation
Textversion	none

A Modified Completeness Theorem of KAT and Decidability of Term Reducibility (Abstract)

Takeo Uramoto
Department of Mathematics, Kyoto University
Sakyo-ku, Kyoto, JAPAN

The main result of this paper is a modified completeness theorem of *KAT*, the equational logic for *Kleene algebra with tests*. This completeness theorem gives an effective reduction of a term reducibility problem to a membership problem of regular languages. In this paper, based on this reduction, we also show that a certain term reducibility problem is decidable.

Background A *Kleene algebra with tests* is a pair $(\mathcal{K}, \mathcal{B})$ of a *Kleene algebra* $\mathcal{K}$ [1] and an embedded Boolean subalgebra $\mathcal{B} \subseteq \mathcal{K}$ whose members are called *tests*. Kleene algebra with tests was introduced by Kozen [2], and the paradigm provides an algebraic approach to program logic and formal verification of program equivalences [2, 3, 4, 7].

From a syntactic viewpoint, the equational logic for Kleene algebra with tests (KAT) is an extension of that for Kleene algebra (KA). Regular expressions (i.e. KA terms) are extended so that, by KAT terms, one can naturally encode simple `while`-programs [2, 3] in such a manner that the encoding is compatible with relational semantics of `while`-programs [6]. Moreover, KAT has a necessary and sufficient set of axioms for reasoning about relational equivalences of programs. That is, an identity $p = q$ between programs (or KAT terms in general) is valid over all relational interpretations if and only if it is formally deducible from the axioms of KAT [5], which we denote by $\mathrm{KAT} \vdash p = q$.

So far, the formal deducibility $\mathrm{KAT} \vdash \phi$ of several forms of formulas ϕ under the axioms of KAT (or other KA variants) and their decision problems have been studied by several authors [5, 8, 9]. It was shown in [5] that $\mathrm{KAT} \vdash p = q$ (i.e. the equational theory of KAT) is decidable. In the case of universal Horn formulas $(\wedge_i p_i = q_i \to p = q)$, the problem is undecidable in general under the axioms of *-continuous Kleene algebras (KAT^*) [5, 8]. However, the case of universal Horn formulas of the form $r = 0 \to p = q$ is proved to be decidable for KA [8] and also for KAT [5], by effectively reducing it to the decision problem of equational formulas.

Our Contribution Continuing this line of investigations of decision problems, the present paper studies the decidability of existentially quantified equational formulas $\exists q \in \mathrm{P}.(p = q)$ in KAT with P being a fixed collection of terms. The problem is to decide if there exists $q \in \mathrm{P}$ such that $\mathrm{KAT} \vdash p = q$ for

a given p. When such $q \in \mathrm{P}$ exists, we say that p is *reducible* to the class P. Also we refer to the problem as the *term reducibility problem*, writing as $\mathrm{KAT} \vdash \exists q \in \mathrm{P}.(p = q)$.

This form of decision problem arises naturally in connection with program optimizations in particular. In program optimization, one is concerned with whether a program p of interest can be refined to another program q that satisfies some fixed criterion (e.g. has PTIME complexity or uses bounded resources), keeping the equivalence of programs. The decision problem of the formula $\exists q \in \mathrm{P}.(p = q)$ concerns the existence of such an equivalent program that satisfies an intended criterion (i.e. the membership in the class P). Finding an equivalent program q for a given program p from a restricted class of programs is a crucial step in KAT-based studies of program optimizations such as [2, 7]. In the present paper, we discuss the decidability of the existence of a desired equivalent program and develop its decision method.

The method of this paper follows the tradition of the algebraic decision methods in combinatorics of regular languages. The key step of this decision method is *pseudo-identity*-based characterizations of combinatorial properties of regular languages (§3). In order to apply the method to term reducibility problems, however, we need to prove a new completeness theorem of KAT (§4). This theorem plays a central role in the reduction of term reducibility problems to combinatorial problems of regular languages, to which the pseudo-identity-based method is applicable. Based on this reduction, we also study an instance of term reducibility problems and show its decidability (§5).

Related work As far as completeness of KAT is concerned, there is a related achievement due to Kozen and Smith [5]. Despite of this achievement, we shall present our completeness theorem, because there is a certain technical problem on the relation between Kozen and Smith's completeness theorem and the pseudo-identity-based decision method.

In [5], Kozen and Smith have shown that KAT is deductively complete with respect to a model of KAT, denoted $\mathcal{G}_{\Sigma,B}$, consisting of *regular sets of guarded strings*. This completeness theorem shows that there is a term interpretation $p \mapsto G(p)$ that assigns effectively to each term p a regular set $G(p) \in \mathcal{G}_{\Sigma,B}$ of guarded strings in such a manner that $G(p) = G(q)$ if and only if $\mathrm{KAT} \vdash p = q$. This theorem provided a counterpart to the well-known completeness theorem of KA: For any regular expressions p and q, $R(p) = R(q)$ if and only if $\mathrm{KA} \vdash p = q$, where $R(p)$ is the standard interpretation of the regular expression p as a regular language. In model-theoretic words, $\mathcal{G}_{\Sigma,B}$ is a free Kleene algebra with tests generated over Σ and B (where B is the extended alphabet of KAT representing tests) in the same way that the algebra $\mathcal{R}_\Sigma$ of regular languages over an alphabet Σ is a free Kleene algebra generated over Σ.

Technically speaking, $\mathcal{G}_{\Sigma,B}$ is given as a subclass of $\mathcal{R}_{\Sigma\cup B\cup\bar{B}}$ simply because regular sets of guarded strings are defined as a certain type of regular languages over an alphabet of the form $\Sigma \cup B \cup \bar{B}$. Due to the completeness of KAT with respect to $\mathcal{G}_{\Sigma,B}$, the term reducibility problem $\mathrm{KAT} \vdash \exists q \in \mathrm{P}.(p = q)$ is equivalent to the decision problem of the membership $G(p) \in G(\mathrm{P})$. Thus, if one could find a decision method for the membership problem in the class $G(\mathrm{P}) \subseteq \mathcal{R}_{\Sigma\cup B\cup\bar{B}}$ of regular languages (i.e. a method of deciding whether or not $L \in G(\mathrm{P})$ for $L \in \mathcal{R}_{\Sigma\cup B\cup\bar{B}}$), then it would follow that $\mathrm{KAT} \vdash \exists q \in \mathrm{P}.(p = q)$ is

decidable.

Characterizations of membership by pseudo identities provide a systematic decision method for this type of decision problem. Schützenberger's theorem [12] is a pioneering result in this direction, from which it follows that the membership problem in the class $\mathcal{SF}$ of *star-free languages* is decidable: A regular language L is said to be *star-free* if there exists an extended regular expression q that contains no Kleene star and $L = R(q)$. Schützenberger proved that a regular language L is star-free if and only if its *syntactic monoid* $M(L)$ satisfies the identity $x^\omega = x^{\omega+1}$ ($\Leftrightarrow \exists n \in \mathbb{N}.\ \forall x \in M(L).\ x^n = x^{n+1}$). A syntactic monoid is a monoid $M(L)$, which is attached canonically to each language L and is finite if and only if L is regular. Since the multiplication table of $M(L)$ is calculable from a regular language L and the equational formula above is decidable by searching the table, it is decidable if a regular language L is star-free (i.e. $L \in \mathcal{SF}$). The key of this decidability proof is that the membership in $\mathcal{SF}$ is characterized by the identity $x^\omega = x^{\omega+1}$ of syntactic monoids. When a class $\mathcal{V}$ of regular languages has such characterizing identities, we say that $\mathcal{V}$ is *definable* by the identities. So far, several decidability results of membership problems were established in a similar way, including the decidabilities for *locally testable languages* [13] and *piecewise testable languages* [14].

However, in a sharp contrast to this line, $\mathcal{G}_{\Sigma,B}$ is not definable by any set of pseudo identities when it is regarded as a subclass of $\mathcal{R}_{\Sigma\cup B\cup\bar{B}}$, as shown in §3. Even worse, every non-trivial subclass $\mathcal{V} \subseteq \mathcal{G}_{\Sigma,B}$ is not definable by any set of pseudo identities. In particular, for any class P of terms, the subclass $G(\mathrm{P}) \subseteq \mathcal{G}_{\Sigma,B}$ is not definable. This undefinability implies that it is essentially impossible to apply the above pseudo-identity-based argument to the decision problem $\mathrm{KAT} \vdash \exists q \in \mathrm{P}.(p = q)$.

The source of this undefinability is that the class $\mathcal{G}_{\Sigma,B}$ is not closed under quotients by finite strings. More specifically, residuals of a guarded string fail to be guarded strings in general.

To remedy this technical issue caused by the undefinability, we introduce the notion of *weakly guarded strings* that relaxes the definition of guarded strings. While in guarded strings test symbols (i.e. letters in $B \cup \bar{B}$) must occur in a definite order and cannot appear twice adjacently, in weakly guarded strings they can occur in an arbitrary order and may be duplicated and also eliminated. Then we define another Kleene algebra with tests, denoted $\mathcal{W}_{\Sigma,B}$, consisting of certain regular sets of weakly guarded strings. We show that KAT is still deductively complete with respect to this refined model $\mathcal{W}_{\Sigma,B}$ as well as $\mathcal{G}_{\Sigma,B}$, but that the class $\mathcal{W}_{\Sigma,B}$ is definable by a set of identities, unlike $\mathcal{G}_{\Sigma,B}$. There is a term interpretation $p \mapsto W(p)$ that assigns effectively to each term p a regular set $W(p) \in \mathcal{W}_{\Sigma,B}$ of weakly guarded strings. This term interpretation W provides an effective reduction of the term reducibility problem $\mathrm{KAT} \vdash \exists q \in \mathrm{P}.(p = q)$ to the membership problem $W(p) \in W(\mathrm{P})$, to which the pseudo-identity-based method is applicable.

References

[1] D. Kozen, "A completeness theorem for Kleene algebras and the algebra of regular events", Infor. and Comput. 110, pp.366–390, 1994.

[2] D. Kozen, "Kleene algebra with tests", Transactions on Programming Languages and Systems, 19(3), pp.427–443, 1997.

[3] D. Kozen, "On Hoare logic and Kleene algebra with tests", Trans. Computational Logic, 1(1), pp. 427–443, May 1997.

[4] D. Kozen, "Nonlocal flow of control and Kleene algebra with tests", Proc. 23rd IEEE Symp. Logic in Computar Science (LICS2008), pp.105–117, June 2008.

[5] D. Kozen and F. Smith, "Kleene algebra with tests: Completeness and decidability.", Proc. 10th Int. Workshop Computer Science Logic (CSL '96), volume 1258 of LNCS, pp.244–259, 1996.

[6] D. Kozen and J. Tiuryn, "Logics of programs", Handbook of Theoretical Computer Science, Elsevier, 1990.

[7] D. Kozen and M. -C. Patron, "Certification of compiler optimizations using Kleene algebra with tests", Proc. 1st Int. Conf. Computational Logic (CL2000), volume 1861 of Lecture Notes in Artificial Intelligence, pp.568–582, 2000.

[8] E. Cohen, "Hypothesises in Kleene algebra", Available from ftp://ftp.bellcore.com/pub/ernie/research/homepage.html, 1994.

[9] E. Cohen, D. Kozen and F. Smith, "The complexity of Kleene algebra with tests", Technical Report TR96-1598, Computer Science Department, Cornell University, July 1996.

[10] L. Polák, "A classification of rational languages by semilattice-ordered monoids", Archivum Mathematium, 40, pp.395–406, 2004.

[11] L. Polák, "On pseudovarieties of semiring homomorphisms", Proc. 29th Int. Conf. Mathematical Foundations of Computer Science (MFPS'04), 2004.

[12] M. -P. Schützenberger, "On finite monoids having only trivial subgroups", Information and Control, 8(2), pp.190–194, 1965.

[13] J. A. Brzozowski and I. Simon, "Characterizations of locally testable events", Discrete Mathematics, 4(3), pp.243–247, 1972.

[14] I. Simon, "Piecewise testable events", Proc. 2nd GI conf., volume 33 of LNCS, pp.214–222, 1975.